UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/848,670	05/04/2001	Shakeel Mustafa	SH0004	7787

7590 09/08/2004

SHAKEEL MUSTAFA
15520 TUSTIN VILLAGE WAY Apt. # 2
TUSTIN, CA 92780

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/848,670	MUSTAFA, SHAKEEL	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because reference number "65" is not pointing to "b_2" as stated in the specification. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 60, 67, 70, 71, 73, 84, 85, 90, 91, 93, 95, 97, 101, 105, 109, 110, 111, 150, 180, 190, 213, 225, 309, 320, 321, 430, 435, 505, 510, 555, 820, 825, 830, 840, 883,

887, 889. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 201. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the step of repeating the encryption rounds "as illustrated in step 221" must be shown or the feature(s) canceled from the claim(s). Also, the existence pf "an inverse function for every function defined" as stated in the second paragraph on page 8 regarding fig.3 must be shown or the feature(s) canceled from the claim(s).No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

5. The drawings are objected to because information segment "S" is not shown in step 215 of fig.9 as stated on page 14 paragraph 2. Also, in fig.4A, it shows M_{min} being greater than $M_{max.}$ Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

6. The disclosure is objected to because of the following informalities: Starting with paragraph 2 on page 8 and then pervading throughout the specification, it is not

understood whether the second pool contains the inverse functions of the functions within the first pool, or that the second pool contains "another class of plurality of functions" with a "unique inverse function for each of the functions defined in the second pool" as stated in the beginning of the paragraph. If the latter is to be understood as written, then the second pool would appear to not have any relationship to the first as suggested throughout the specification and fig.3. However, in either case, as stated above, the claimed subject matter of there being a inverse function for every function defined in the pool is not shown in fig.3, which only adds to the confusion.

On page 9 paragraph 3, it is not understood how M_{min} can be greater than M_{max}.

On page 10 paragraph 2, fig.5A shows the Function Bit entries as being "Group #0" and in the specification it states that the entries are "Group #1).

Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 2-20 rejected under 35 U.S.C. 101 because theses claims are directed to neither a process nor a machine, but rather embraces or overlaps two different statutory classes of invention set forth in 35 U.S.C. 101.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 2-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims that claim both method and system steps of using an apparatus are indefinite under 35 U.S.C. 112 second paragraph.

11. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-22 are method claim that contain no method steps. The use of the phrase "means for" implies that these are apparatus claims.

12. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-22 recite numerous limitations such as: "the first pool", "the second pool", "the numeric value of step (b)", "the digital information

segment", "the second function pool as described in step d", "the arbitrary bit segment", "the first pool as described in step c", "the seed arbitrary binary bit segment", "the said arbitrary binary bit segment", "the corresponding inverse function", "said method for operating a digital information processing system that decrypts information", "the encrypted seed binary bit segment", "the first outcome", "the second outcome", and "the seed random number". There is insufficient antecedent basis for this limitation in the claim.

13. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The terms "any length", "any type", and "any complexity" in claim 1 are relative terms which render the claim indefinite. These terms are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The term "large" in claim 5 is a relative term which renders the claim indefinite. The term "large" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The term "any type" in claim 15 is a relative term which renders the claim indefinite. The term "any type" is not defined by the claim, the specification does not

provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The term "any information" in claim 19 is a relative term which renders the claim indefinite. The term "any information" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The terms "any type", "any arbitrary length segment", and "any information means" in claim 21 are relative terms which render the claim indefinite. These terms are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The term "any means mutually agreed" in claim 22 is a relative term which renders the claim indefinite. The term " any means mutually agreed " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 15 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. There are no teachings pertaining "receiving a public key from the host processor" and encrypting system information using "the public key of the host processor". There also is no teachings of decrypting the received information using "the host's private key".

Claim Objections

Claim 1 is objected to because of the following informalities: in the limitation "means for defining a plurality of function pool", the word "pool" needs to be plural.

In claim 2 element (f), change "functions entries" to "function entries".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson et al (US pat 6,052,469).

Regarding claim 1, Johnson teaches a method for operating a digital information processing system that encrypts information from a plurality of remote processors to a host processor or vice versa the method comprising processor executed steps of:

at the host and the remote processors before the start of encryption procedure:

means for assigning and mutually agreeing upon, a pre-determined number of bits that are located at pre-determined and specific positions, called Group and Function Bits, within a seed binary bit segment consisting of any length (col.8 lines 56-61; col.12 lines 19-30);

means for defining a plurality of function pool containing any type of mathematical or logical functions of any complexity (col.5 lines 62-67; col.18 lines 48-62);

means for establishing a unique relationship between the functions defined in the first pool with the functions defined in the second pool sequentially identical at both the host and the remote processors (col.13 lines 17-30; col.18 lines 48-62);

means for defining a number 'N' which indicates the total number of rounds used for encryption/decryption process (col.17 lines 1-11).

at the remote processor:

(a) means for generating and sending a seed arbitrary binary bit segment consisted of any length to the host processor (col.13 lines 19-24);

(b) means for processing the seed arbitrary binary bit segment at the remote processor (col.13 lines 17-30);

(c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment (col.13 lines 17-30);

(d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (b) (col.14 lines 42-55);

(e) means for identifying the corresponding single or plurality functions from the second pool (col.14 lines 45-47);

(g) means for encrypting the digital information segment through operating single or plurality of mathematical or logical functions selected from the second function pool as described in step d (col.18 lines 54-62);

(f) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step c (col.5 lines 62-67);

(h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment (col.16 lines 46-58; col.17 lines 47-50); and

(i) means for repeating the steps (b) to (h) N' times and then transmitting the resulting encrypted digital information segment to the said host (col.17 lines 1-11).

Regarding claim 21, Johnson teaches a method for operating a digital information processing system that encrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of:

at the transmitting device:

means for generating a seed random number consisting of any arbitrary length and transmitting the said random number to the receiving device (col.12 lines 39-49);

means for using the information contained in the random number to identify single or plurality of unique mathematical or logical functions identical at the both transmitting and the receiving devices (col.14 lines 42-55);

means for encrypting any type of digital information consisted of any arbitrary length segment through operating the mathematical or logical functions (col.12 lines 19-25);

means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round (col.16 lines 46-58; col.17 lines 47-50);

means for identifying the number of encryption rounds, N, through the use of any information means mutually agreed between the transmitting and the receiving devices (col.17 lines 1-11); and

means for repeating the encryption process on the said digital information segment and the said random number for N number of rounds (col.16 lines 46-58; col.17 lines 1-11; col.17 lines 47-50).

Regarding claim 22, Johnson teaches a method for operating a digital information processing system that decrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of:

at the receiving device:

means for receiving and identifying the seed random number of an arbitrary length from the transmitting device;

means for identifying the number of encryption rounds, N, through any means mutually agreed between the transmitting and the receiving devices (col.17 lines 1-11);

means for using the information contained within the specific bits of the seed random number to identify a single or plurality of unique mathematical or logical functions (col.14 lines 45-47);

means for identifying single or plurality of inverse functions corresponding to each of the identified mathematical or logical functions (col.8 lines 11-40);

means for decrypting the received digital information segment through operating single or plurality of inverse functions (col.8 lines 11-40);

means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round (col.16 lines 46-58; col.17 lines 47-50); and

means for repeating the decryption process on the received digital information segment for N number of rounds to remove any effects of encryption on the said digital information segment (col.8 lines 37-40; col.16 lines 46-58; col.17 lines 1-11; col.17 lines 47-50).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Andrew Caldwell
Andrew Caldwell

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

August 25, 2004